Technical Cybersecurity

Exploit Kits

Defined

Exploit kit

- A collection of exploits that targets a particular piece of software, usually packaged with a tool or group of tools that allow the exploits to be triggered.
- Commonly used to refer to *Browser Exploit Kits*

Many exist

- And they are essentially Platforms-as-a-Service
- Different exploit kits compete for customers
- Provide control panels and customer service

Activity as of Fall 2018

Top exploit kits

- **Fallout**: Newest, based on Nuclear; mutating URI paths
- **Rig**: A classic, losing market to Fallout; strongest exploits
- **Grandsoft**: Uses compromised websites as intermediaries
- **Magnitude**: Targets Asia
- **Underminer**: Delivers a bootkit, not ransomware!

Top exploited vulnerabilities & Payloads

- CVE-2018-8174 and CVE-2018-4878
- Miners were popular, moving back to ransomware or bootkits

Exploits

Current popular exploits

- CVE-2018-8174: Memory handing problem with objects in memory in the Windows VBScript Engine; RCE
- CVE-2018-4878: Memory handing issue (use-after-free) in Adobe Flash; RCE

Exploits change over time

- These are reasonably new (e.g. 5-8 months old)
- Exploits used are updated regularly

Typical Attack Sequence

Browser lands on compromised site

- Compromised website or malvertising page
- …or a compromised website that delivers malvertising

Redirect chain

- A sequence of redirecting websites
- Not always used

Landing page

- Loads exploits based on browser and browser configuration
- Executes exploits and injects malware

Next, phishing.